DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer / G-6

1 Aug 02

SAIS-EIG

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Knowledge Management Guidance Memorandum Number 2 Implementing Instructions

1. The Secretary of the Army (SA) and the Chief of Staff, Army (CSA) signed the Army Knowledge Management (AKM) Guidance Memorandum Number 2 on June 19, 2002. This memorandum identified accelerated, increased levels of performance to move our Army closer to becoming a network-centric, knowledge-based force. The purpose of this memorandum is to provide additional information in support of your efforts to execute the new requirements from our senior leadership.

2. Implementing instructions (attached) for executing the accelerated requirements are provided for the following areas:

a. Goal 2 - Business Initiatives Council

b. Goal 3 - Baseline assessments and server consolidation

c. Goal 4 - Reduction and webification of applications

d. Information assurance status and initiatives

3. The Army Knowledge Online (AKO) is the primary portal for Army unclassified intranets and the AKO email address should be used on all official correspondence. All functional database applications that include an email address should use the AKO/AKO SIPRNet (S) email address. The AKO-S serves as the primary portal for Army classified intranets and the SIPRNet. Any individual required to use the SIPRNet should have an AKO-S account.

4. The AKM Goal 1 implementing instructions for fiscal year 2003 and beyond will focus on tracking the command, control, communications and computers/information technology (IT) resource implications of the server consolidation, application reduction and other business initiatives as listed in the AKM Guidance Memorandum Number 2. Additionally, Goal 1 will continue to monitor non-Chief Information Officer managed IT expenditures. Updated procedures will be published separately by early-mid August 2002.

5. The progress made toward achieving a transformed Army is the result of the hard work each of you accomplished over the last ten months. I ask that you continue your efforts, maintain focus, and move us closer to achieving our goal of a network-centric, knowledge-based force. Our achievements are impacting soldiers today - we must continually assess our accomplishments and move forward with urgency.

4 Attachments

PETER M. CUVIELLO
Lieutenant General, GS
Chief Information Officer/G-6

DISTRIBUTION:
Under Secretary of the Army
Vice Chief of Staff, Army
Sergeant Major of the Army
Assistant Secretary of the Army (Acquisition, Logistics and Technology), ATTN: SALT
Assistant Secretary of the Army (Civil Works), ATTN: SACW
Assistant Secretary of the Army (Financial Management and Comptroller), ATTN: SAFM
Assistant Secretary of the Army (Installations and Environment), ATTN: SAIL
Assistant Secretary of the Army (Manpower and Reserve Affairs), ATTN: SAMR
General Counsel, ATTN: SAGC
Administrative Assistant to the Secretary of the Army, ATTN: SAAA
Chief Information Officer/G-6, ATTN: SAIS-ZA
The Inspector General, ATTN: SAIG-ZA
The Auditor General, ATTN: SAAG-ZA
Deputy Under Secretary of the Army, ATTN: SAUS
Deputy Under Secretary of the Army (Operations and Research), ATTN: SAUS-OR
Chief of Legislative Liaison, ATTN: SALL
Chief of Public Affairs, ATTN: SAPA-ZA
Director, Small and Disadvantaged Business Utilization, ATTN: SADBU
Director of the Army Staff, ATTN: DACS-ZD
Deputy Chief of Staff, G-1, ATTN: DAPE-ZA
Deputy Chief of Staff, G-2, ATTN: DAMI-ZA
Deputy Chief of Staff, G-3, ATTN: DAMO-ZA
Deputy Chief of Staff, G-4, ATTN: DALO-ZA
Deputy Chief of Staff, G-8, ATTN: DAPR-ZA
Assistant Chief of Staff for Installation Management, ATTN: DAIM-ZA
Chief of Engineers, ATTN: DAEN-ZA
(CONT)

DISTRIBUTION: (CONT)
The Surgeon General, ATTN: DASG-ZA
Chief, National Guard Bureau, ATTN: NGB-ZB
Chief, Army Reserve, ATTN: DAAR-ZA
The Judge Advocate General, ATTN: DAJA-ZA
Chief of Chaplains, ATTN: DACH-ZA

Commander
U.S. Army Europe and Seventh Army, ATTN: AEACG
Eighth U.S. Army, ATTN: EACG
U.S. Army Forces Command, ATTN: AFCG
U.S. Army Training and Doctrine Command, ATTN: ATCG
U.S. Army Materiel Command, ATTN: AMCCG
U.S. Army Corps of Engineers, ATTN: CECG
U.S. Army Special Operations Command, ATTN: AOCG
U.S. Army Pacific, ATTN: APCG
U.S. Army Intelligence and Security Command, ATTN: IACG
U.S. Army Military Traffic Management Command, ATTN: MTCG
U.S. Army Criminal Investigative Command, ATTN: CICG-ZA
U.S. Army Medical Command, ATTN: DASG-ZA
U.S. Army Military District of Washington, ATTN: ANCG
U.S. Army South, ATTN: SOCG
U.S. Army Test and Evaluation Command, ATTN: CSTE
U.S. Army Space and Missile Defense Command, ATTN: SMDC-ZA

Superintendent, U.S. Military Academy, ATTN: MASP

Program Executive Officers
Air and Missile Defense
Ammunition
Aviation
Command, Control, and Communications - Tactical
Chemical and Biological Defense
Combat Support and Combat Service Support
Enterprise Information Systems
Ground Combat Systems
Intelligence, Electronic Warfare and Sensors
Soldier
Tactical Missiles
Simulation, Training and Instrumentation Command
Information Systems
(CONT)

DISTRIBUTION: (CONT)
Program Managers:
Chemical Demilitarization
Joint Simulation Systems
Missile Defense Agency

IMPLEMENTING INSTRUCTIONS FOR GOAL 2
Business Initiatives Council (BIC)

1. Purpose. To provide implementing instructions for participation in the Army Business Initiatives Council (ABIC) process. The ABIC is a forum for the development and promulgation of best practices across the enterprise and meets the intentions of AKM Goal 2 to *"integrate knowledge management and best business practices into Army processes."* AKM Guidance Memorandum Number 2, dated 19 June 2002, states that *"Your active participation in these forums is essential to the success of Army Transformation and AKM."*

2. Guidance Proponent. The Army G-8 is the HQDA proponent for the ABIC and the Deputy Army G-8, Dr. Craig College, serves as the ABIC Executive Director. The CIO/G-6 ABIC lead, and POC for this implementation guidance, is COL Jane Maliszewski, Director Strategic Outreach, 703-604-2068, DSN 334-2068, jane.maliszewski@us.army.mil.

3. The Army Business Initiatives Council (ABIC).

a. General: The ABIC was formed by the SECARMY in October 2001 with the mission of improving the Department of the Army's business operations and processes. The streamlined ABIC approval process is intended to identify and expeditiously implement business practices supporting more effective operations and better use of financial and human resources. The overarching objective recognizes that process improvements made through the ABIC will ultimately enhance the quality of life, operational excellence, and improved support to the warfighter. The ABIC solicits, assesses, and implements great ideas that:

- Improve or streamline processes by implementing best practices, applying technology, and exploring new ways of doing business
- Eliminate processes with no added value
- Eliminate burdensome and unnecessary rules and regulations
- Adopt better tools to do our jobs
- Offer longer range reform opportunities (by pursuing regulatory or legislative changes)

b. The goal is to improve processes by identifying best practices that can be adopted throughout the Army and may be considered for promulgation throughout the Department of Defense. As an incentive, organizations retain a portion of the savings they generate from implementing an ABIC initiative. The ABIC solicited suggestions from the Army staff and MACOMs on 11 Feb 02. That first round generated 27 proposals, of which 16 were approved for implementation by the SECARMY on 8 May 02. The Round 2 proposal request of 23 May 02 generated an additional 27 initiatives.

4. Organization of the ABIC:

a. The Army Executive Steering Committee (AESC): Chaired personally by the Secretary of the Army, the AESC has representatives from each staff and functional area (Assistant Secretary of the Army and Deputy Chief of Staff level). The AESC decides on the disposition of each initiative submitted and is briefed on status of their implementation plans each quarter. Additionally, the AESC forwards initiatives with DoD-wide applicability to the DoD Business Initiatives Council.

b. Army Process Functional Boards (PFB): Six Process Functional Boards (PFB) review, propose, and coordinate all ABIC initiatives. The six PFBs are: Manpower and Personnel, Installations and Logistics, Resource Management; Information Technology; Acquisition Management; and Test and Evaluation.

c. Army BIC Support Team: The Army BIC Support Team is the focal point for receiving and reviewing new initiatives and provides staffing support to the AESC and PFBs. The ABIC Support Team has established an ABIC homepage on AKO (www.us.army.mil: AKO/Army Communities / Financial / ABIC). The point of contact is Mr. Brian Murray, G-8, (703) 692-5270, brian.murray@us.army.mil.

d. IT Process Functional Board (IT PFB): The Army CIO/G-6 runs the IT PFB to coordinate all IT and IT-enabled initiatives through the ABIC process. The CIO/G-6 IT PFB support team is: Mr. Steve Billingsley (703) 604-2051, stephen.billingsley@us.army.mil, and Mr. John Medve (703) 602-2063, john.medve@us.army.mil.

5. New Initiative Submission and Staffing Process. The SECARMY has established a quarterly cycle for submission of ABIC initiatives. This cycle consists of four phases and is initiated by an e-mail memorandum from the Army G-8 requesting new initiatives and designating timelines.

a. Phase I: Initiative Submission *(30 days).* HQDA Staff and MACOMs are required to submit one ABIC initiative per cycle as specified by Army G-8 guidance. The initiatives must have general officer/SES concurrence. Initiatives will be submitted via the database template found on AKO/Army Communities / Financial / ABIC *(requires submitter/contact for the initiative to apply for userid/password from the site administrator).* Step by step instructions are found in paragraph 6d of this document. The ABIC Support team processes the initiative and then assigns it to one of the six Process Functional Boards (PFB) for review and staffing.

b. Phase II: Initiative Staffing *(30 days)*. Each PFB has its own procedure for staffing new initiatives. The IT PFB relies on both the CIO Executive Board (CIO EB) and the internal CIO/G-6 IT PFB Review Group to review all IT and IT-enabled initiatives to ensure consistency with the Army Knowledge Management strategy. Army CIO EB members are notified of initiatives ready for review via the Army CIO Executive Board website. Members will access the ABIC Database (instructions in paragraph 6d) to view the initiatives then either email their comments on each initiative directly to Mr. Steve Billingsley at stephen.billingsley@us.army.mil or submit them for inclusion into the MACOM review, as determined by their ABIC MACOM POC.

c. Phase III: ABIC Executive Steering Committee Review *(1 day).* At the completion of the staffing process the Army Executive Steering Committee (AESC), chaired by the SECARMY, is briefed on each initiative. At this meeting, initiatives are approved, disapproved or deferred for more development. A champion for approved initiatives is assigned.

d. Phase IV: Implementation Plan Development *(30 days).* Champions of approved ABIC initiatives will develop implementation plans that are approved by the ABIC Executive Director (Deputy Army G-8) and PFB Chairs. Template for the implementation plan is on www.us.army.mil AKO homepage/Army Communities/Financial/ABIC/ABIC Knowledge Center. Status and significant milestones of the implementation plans are briefed to the SECARMY quarterly.

6. Executing These Implementing Instructions

a. Defining "Best Practices": The ABIC is looking for best practices that are appropriate for deployment across the Army enterprise. A best practice is a documented strategy, tactic, or process used by business, government, or organizations to achieve specific results, typically better ways of operating, reducing the costs of a function/process, and/or achieving superior performance. In the Army, we are targeting two approaches to best practices: enterprise-wide and local-use.

(1) Enterprise-wide Best Practices: A practice that 'makes sense' to do across the Army to provide a consistent, end-to-end processes that improve productivity, generates cost savings, or enhances operational efficiency. For example, "Streamline the Army Publications Process" is an ABIC proposal that affects operations across the enterprise. This proposal uses the 'best practice' of incorporating collaborative processes to re-engineer and streamline the existing procedure that will result in measurable improved cycle times for document publication. Enterprise-wide best practices can be general administrative procedures, such as those affecting the publications process, or a 'best practice' in a particular functional area that will apply across the Army, such as the IT initiative of Enterprise Configuration Management or the Test and Evaluation Board initiative of piloting Limited Liability Companies.

(2) Local Best Practices: A method of accomplishing a business function or process within a certain area that is considered superior to all other known methods, but is not necessarily applicable for enterprise-wide deployment. Local best practices provide ideas, models, and benchmarks for others to use to improve their operations using proven solutions. The AKM Goal 2 Best Practice database contains many examples of local best practices that use knowledge management concepts to improve performance. The site can be accessed from the AKO Knowledge Collaboration Center *(Army Communities/Army CIO G-6/AKM/Best Practice Inventory)*. An example of a local best practice that was

considered by the ABIC is "RM Online," a resource management tool that the Army Materiel Command uses to track resource management within their MACOM. The ABIC decided it was a 'best practice' that other commands should consider, but was not applicable for Army-driven enterprise-wide deployment.

b. Influence of Best Practices on ABIC: The ABIC proposals generally fall into two categories: a process that an organization has adopted and used with proven success that could be deployed across the Army/functional enterprise or a proposal to streamline an existing process by using best practices identified from elsewhere. An example of the former is the Automated Systems Intelligence Database (ASID) that is already in use within the G-2/INSCOM community and is now being evaluated for deployment Army-wide as part of the Enterprise Configuration Management initiative. The "World Class Civilian Hiring Process" is an example of the improvement of an existing process with the use of best practices from the corporate human resources area.

c. ABIC Contributions: Each HQDA staff and MACOM will be tasked by the Army G-8 to contribute at least one proposal for the ABIC each quarter, but the process is also open to commands throughout the Army. If you have a process that works, or recognize that a process can be improved, and believe it is applicable for Army-wide deployment; you are invited to submit it as an ABIC initiative. The key component of the proposal should focus on eliminating, changing, or improving a process, not on the technical solution, such as a type of software. The solution can be highlighted as an example of how the process can be improved, but the need for a consistent and refined process, not the toolset, is the basis for the initiative. All contribution must be supported by a general officer/SES. Contact the ABIC Support team for more information (see paragraph 4c.)

d. Submitting a New Initiative:

(1) Log on to Army Knowledge Online (AKO)
(2) On the AKO Home Page, look down the left side of the page and click on 'Army Communities'
(3) Click on 'Financial / ABIC'
(4) Locate the BIC Initiative Submission main page (to the right of Dr. Craig College's picture)
(5) Log on to the ABIC Initiative Submission Database
- *(if you don't have a userid/password, click on 'Sign Up For an Account' to register)*

(6) Click on the "New" tab and fill in the required fields
- *(if you are reviewing an initiative, click on the circle next to the initiative title then on the 'View' tab at the top of the page)*

NOTE: A General Officer/SES must approve your submission prior to entering it in the ABIC Initiative Submission Database.

e. **Reviewing Initiatives:**

(1) The ABIC Executive Director will request a review of all initiatives by the designated ARSTAFF and MACOM ABIC POC. Clarification of proposals can be coordinated directly through the appropriate ABIC Process Functional Boards. A complete ABIC Point of Contact list is located on the ABIC AKO Collaboration Site under the ABIC Support Team Knowledge Center. The initiatives are located on the AKO/ABIC web page by following the same steps as above to access the ABIC database, selecting an initiative to view and hitting the VIEW Tab at the top of the page. The database does not currently log comments, so these must be emailed to the Army G-8 ABIC Support Team or to the applicable ABIC Process Functional Board POC. Classify your recommendation/review into one of the five categories below:

(a) **GO-Army Only**: An Army-unique process; makes sense to have a consistent process Army-wide. Recommend approval of this initiative for Army enterprise use.

(b) **GO-Army and DOD:** Recommend approval for Army use, but is applicable as a DoD-wide process (include explanation of why you believe it should be implemented DoD-wide).

(c) **Already in Play**: Initiative is duplicative of an existing Army program (include an explanation as to rationale and listing of on-going programs that you feel meet the initiative intent).

(d) **Disapprove w/Comment**: Initiative should not be implemented. Does not make sense to adopt as an Army-wide standard process. Include detailed explanation.

(e) **Discuss w/Comment**: Specific issues should be discussed/resolved before final determination can be made. Include detailed explanation of issues you believe must be resolved prior to making final decision.

(2) All initiatives and staffing recommendations are presented to the SECARMY at the quarterly AESC meeting.

(3) Questions concerning IT initiatives should be directed to the CIO/G-6 IT PFB Support team (paragraph 2). Questions concerning all other initiatives should be referred to the ABIC Support team, Mr. Brian Murray, ABIC Support Staff, paragraph 4c.

IMPLEMENTING INSTRUCTIONS FOR GOAL 3
Baseline Assessments and Server Consolidation

1. **Purpose**. To provide implementing guidance for Goal 3 of the Army Knowledge Management (AKM) Strategic Plan as directed by Army Knowledge Management Guidance Memorandum Number 2, signed by the Secretary of the Army and the Chief of Staff, Army on 19 June 2002. The guidance provided toward achieving Goal 3, managing the infostructure at the enterprise level, is as follows:

a. Effective immediately, HQDA functional proponents, Major Army Commands (MACOMs), and Regional Installation Management Directors (stood up by 1 October 2002) will step up their efforts to consolidate servers on their posts, camps, and stations. The end state goal is to reduce the number of servers supporting the Army business and installation communities by an additional 30 percent by the end of Fiscal Year 2003 from the September 2001 baseline.

b. By 1 August 2002, all HQDA functional proponents and MACOMs will submit a report to the Army CIO stating their plans for server consolidation. Thereafter, HQDA functional proponents, MACOMs, and Regional Installation Management Directors will provide progress reports at Army CIO Executive Board meetings.

2. **Guidance Proponent**. The Army Chief Information Officer (CIO) is the HQDA proponent for implementation of this guidance. The points of contact within the Information Infrastructure Modernization (IIM) Division in the Information Operations, Networks and Space Directorate of the Army CIO/G-6 are Chief, IIM Division, COL Mark Barnette, 703-602-7210, DSN 332-7210, mark.barnette@us.army.mil and IIM Staff Action Officer, Ms. Patricia Bodenstein, 703-602-7517, DSN 332-7517, patricia.bodenstein@us.army.mil.

3. **Definitions**.

a. Business Case Analysis. A management planning and decision-making tool that is used to define alternative ways of doing business and the associated investment and operating costs, savings, payback period, and return on investment. The analysis includes the rationale and methodology for quantifying benefits and costs to include a discussion of critical success factors and risk assessment.

b. Enterprise. An action, activity, program or effort, such as technology, that is appropriate across the Army and includes the Active Component, the Reserves, the National Guard, civilians, and selected contractors.

c. Infostructure. The information technology (computers, ancillary equipment, software, architecture, security, communications, programs, facilities, services, and related resources) required to support the network centric, knowledge based Army.

4. **Roles and Responsibilities.**

a. The Army CIO will:

1) Act as the functional proponent for all enterprise infostructure initiatives such as Windows 2000, Active Directory, Information Assurance, server consolidation, network management, Public Key Infrastructure, Biometrics, and Common Access Card to include their related program requirements, resources, and policies.

2) Lead working group(s) with representation from HQDA functional proponents, MACOMs, and Regional Installation Management Directors to develop an enterprise management and consolidation strategy to include the enterprise architectures for the Army's infostructure.

3) Through the Network Enterprise Technology Command (NETCOM), act as the Army's single authority to operate and manage the enterprise infostructure. NETCOM will have technical command and control for the Army's critical networks and systems.

b. The Army CIO Executive Board will:

1) Validate infostructure requirements for development and implementation.

2) Identify and resolve issues relating to enterprise infostructure programs.

3) Oversee performance of the functions, initiatives, and programs within the enterprise infostructure.

c. The Program Executive Officer for Enterprise Information Systems (PEO EIS) will:

1) Serve as the material developer and systems integrator for the consolidation of the enterprise infostructure.

2) In coordination with the Army CIO, lead development of the business case analysis for Windows 2000/Active Directory and server consolidation to include, if directed, the supporting Request for Proposal and follow-on implementation.

d. The Program Executive Officer for Command, Control and Communications-Tactical and the U.S. Army Communications Electronics Command will act as the technical integrator and material developer for deployable command, control and communications systems which affect the enterprise infostructure.

e. The HQDA functional proponents, MACOMs and Regional Installation Management Directors (stood up by 1 October 2002 under the Assistant Chief of Staff for Installation Management) will:

1) Accelerate consolidation of email, web, file, domain controller, and print servers (to include application servers) on their posts, camps, and stations in accordance with the following guidelines:

a) The Director of Information Management (DOIM) on each post will consolidate servers for Army tenants residing on the post to a minimum number of server cluster locations; for example, one server cluster supporting the main post and one server cluster supporting the hospital. Tenants currently associated with other Army networks (e.g., ARNet, GuardNet, IGNET) that encompass multiple posts will remain within their networks.

b) All Army tenants on a post will assist the DOIM in consolidating servers to those locations specified by the DOIM. DOIMs will coordinate with their Installation Commander and Army tenants to develop the requisite Memorandums of Agreement to provide the resources needed to support server consolidation.

c) DOIMs should consider Continuity of Operations, network access, and facility improvements (e.g., back-up power, HVAC, storage) required to support server consolidation with enhanced system availability and reliability.

d) Army tenants moving their mail services to the installation consolidated mail servers will use the post Simple Message Transport Protocol (SMTP) gateway naming convention (firstname.lastname@ post.army.mil). Tenants using alternate naming conventions (e.g., @tenant.post.army.mil) may maintain that name space by modifying their mail exchange record to direct mail to the post consolidated SMTP mail gateway. If there are technical, cost, or customer service ramifications in adhering to this guidance, the DOIM is authorized to determine the interim naming convention and migration strategy.

e) DOIMs must allow all mail and application systems to coexist within consolidated facilities, as this guidance does not mandate consolidation on any specific vendor product.

f) All personnel who register for a "universal" Army Knowledge Online (AKO) email account will have the ability to use the growing capabilities of the AKO to access information throughout their career. Personnel requiring access to the Secure Internet Protocol Router Network (SIPRNET) will obtain an AKO SIPRNET (AKO-S) account.

g) When registering on AKO or AKO-S, there is a capability to automatically forward mail to the user's email address on the post mail server. It is not recommended users operate locally from their AKO email account on a daily basis. The current communications infrastructure is not sufficient to handle the large volume of email traffic, particularly when the majority of email traffic is not transmitted out of the local service area. Registering on AKO, however, supports the Army enterprise registry required for network and knowledge centric capabilities and concepts enabling Army transformation.

2) Report their plans for server consolidation to the Army CIO by 1 August 2002. The format for server consolidation plans is enclosed.

3) Provide quarterly progress reports at the Army CIO Executive Board meetings on the status of their server consolidations in accordance with the enclosed format.

Thereafter, progress status will be submitted through the Key Performance Metrics Monitor and Strategic Readiness System once the Army CIO, in coordination with the Assistant Secretary of the Army (Financial Management & Comptroller) and the G-3, establishes the reporting process.

5. **Process**. The Army CIO, in coordination with PEO EIS, is in the process of defining the service requirements, standard performance measures, systems architecture, and acquisition strategy for managing the Army enterprise networks and applications. In January 2002, the Army Enterprise Infostructure Management Steering Group was formed under the oversight of the Army Chief Information Officer Executive Board to facilitate implementation of the enterprise strategy. In addition, a collaboration site was established under the AKO web page to improve communications and planning efforts. As part of the HQDA realignment, NETCOM was established under the Army CIO as the single agency responsible for the operation and management of the Army enterprise infostructure. NETCOM is developing the Concept of Operations for the enterprise management of the infostructure that will enable the Army to reduce costs of operations, obtain better configuration management control, and facilitate adoption of best business practices. In addition, several server consolidations are being implemented within the Military District of Washington and Europe to demonstrate enterprise processes and technologies as well as document lessons learned for Army-wide implementation. Pending further refinement of the Army enterprise infostructure strategy, projects such as server consolidation need to be accelerated to achieve the Army enterprise vision. Consolidation efforts even at the installation level will facilitate and enable future migrations to a regional strategy, if deemed appropriate. Agencies must be flexible and ready to make any necessary adjustments as more detailed guidance emerges on the objective end-state architecture.

6. **Metrics**.

a. Track HQDA functional proponent and MACOM responses to 1August 2002 suspense for server consolidation plans.

b. Monitor quarterly status updates submitted by HQDA functional proponents and MACOMs/Regional Installation Management Directors on server consolidations.

Server Consolidation Plan Report Format and Content
(one plan per post, camp, or station)

HQDA functional proponents and MACOMs will submit the following information electronically to the Army CIO/G-6 not later than 1 August 2002 using the online web application located at https://goal3.jdp.us.army.mil/goal3/registerplan.aspx. Figure 1 provides a sample view of the server consolidation plan web application. The G-6 point of contact is Ms. Patricia Bodenstein, commercial 703-602-7517, DSN 332-7517, email: patricia.bodenstein@us.army.mil.

1. MACOM/HQDA functional proponent (e.g., TRADOC, AMC, SAALT, G1).

2. ACSIM/NETCOM region (e.g., NE, NW, SE, SW).

3. Post, camp, or station.

4. DOIM point of contact (name, office address, phone, email).

5. Number of users on the post, camp, or station.

6. Number of servers (baseline and end-state) for each of the following: email, web, file, print, domain controllers, and applications.

7. Implementation schedule (total number of servers to be eliminated on a quarterly basis for 4QFY02, 1QFY03, 2QFY03, 3QFY03, 4QFY03). 4QFY02 may reflect consolidations completed to date with baseline information adjusted accordingly.

8. Return on investment (estimated annual savings or cost avoidance) in terms of reduced hardware, software, system operations and administration, facility costs (show dollar amount).

9. List of participating activities to include any non-participating activities, point(s) of contact, and supporting justification.

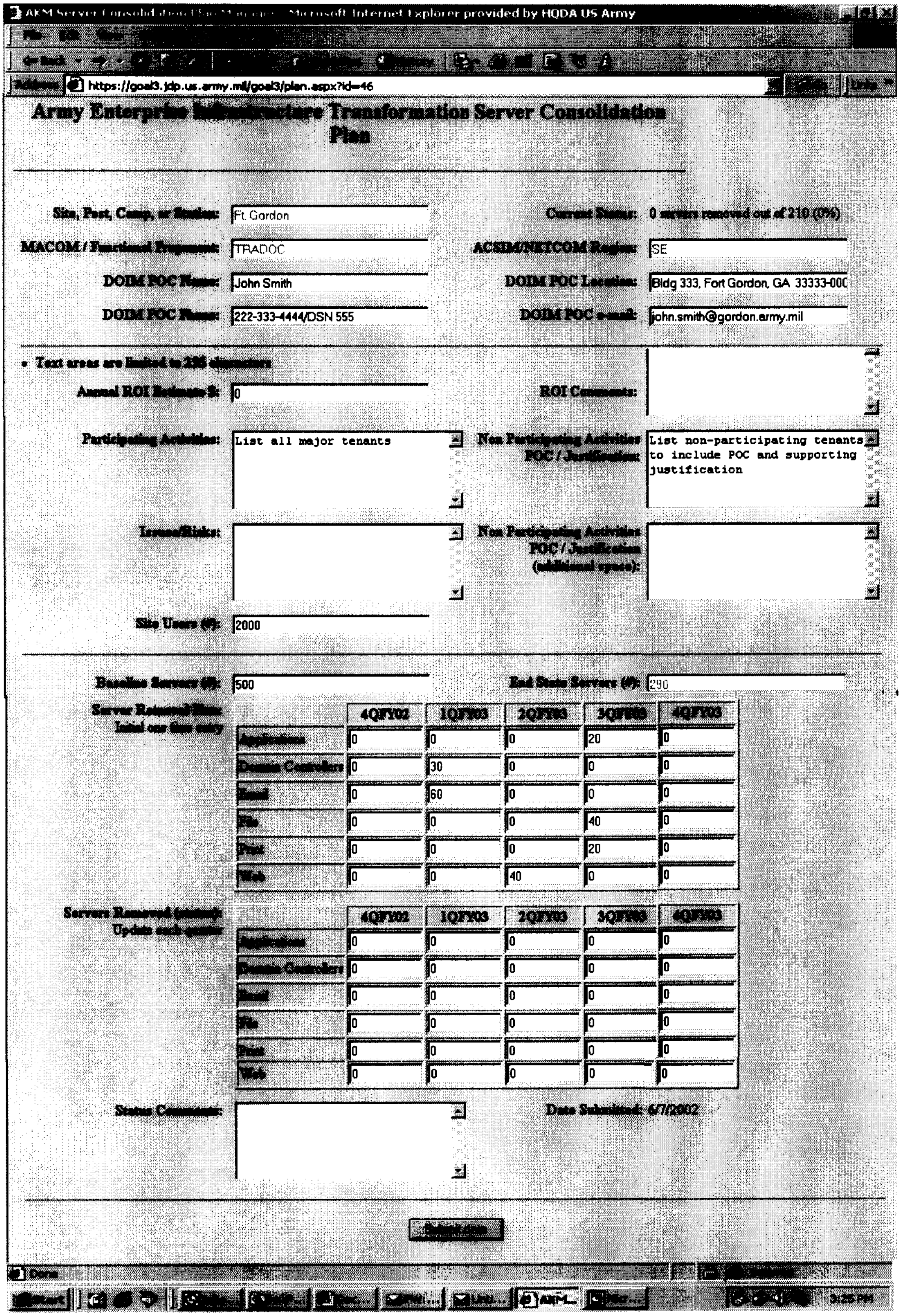
10. Issues/Risk assessment (e.g., lack of cooperation, investment, leadership support)

Quarterly Update Report Format and Content

On a quarterly basis beginning 15 October 2002, HQDA functional proponents and MACOMs/Regional Installation Management Directors will use the above online web application to report the actual number of servers eliminated during each fiscal year quarter. Status of server consolidations will then be made available to senior Army leadership using the following format.

Installation	Baseline Number of Servers	Number of Servers Eliminated To Date	Total Number of Servers to be Eliminated	End-State Number of Servers	Estimated Annual Savings/ Cost Avoidance

Enclosure


AKM Server Consolidation Plan Manager - Microsoft Internet Explorer provided by HQDA US Army
File
Edit
View
Back
History
Address
https://goal3.jdp.us.army.mil/goal3/plan.aspx?id=46
Go
Links
Done
Start
AKM...
3:25 PM

Army Enterprise Infrastructure Transformation Server Consolidation Plan

Site, Post, Camp, or Station:	Ft. Gordon	Current Status:	0 servers removed out of 210 (0%)
MACOM / Functional Proponent:	TRADOC	ACSIM/NETCOM Region:	SE
DOIM POC Name:	John Smith	DOIM POC Location:	Bldg 333, Fort Gordon, GA 33333-000
DOIM POC Phone:	222-333-4444/DSN 555	DOIM POC e-mail:	john.smith@gordon.army.mil

- Text areas are limited to 255 characters

Annual ROI Estimate $:	0	ROI Comments:	
Participating Activities:	List all major tenants	Non Participating Activities POC / Justification:	List non-participating tenants to include POC and supporting justification
Issues/Risks:		Non Participating Activities POC / Justification (additional space):	
Site Users (#):	2000		
Baseline Servers (#):	500	End State Servers (#):	290

Server Removal Plan: Initial one time entry

	4QFY02	1QFY03	2QFY03	3QFY03	4QFY03
Applications	0	0	0	20	0
Domain Controllers	0	30	0	0	0
Email	0	60	0	0	0
File	0	0	0	40	0
Print	0	0	0	20	0
Web	0	0	40	0	0

Servers Removed (status): Update each quarter

	4QFY02	1QFY03	2QFY03	3QFY03	4QFY03
Applications	0	0	0	0	0
Domain Controllers	0	0	0	0	0
Email	0	0	0	0	0
File	0	0	0	0	0
Print	0	0	0	0	0
Web	0	0	0	0	0

Status Comments:

Date Submitted: 6/7/2002

Submit data

Figure 1. Sample View of the Server Consolidation Plan Web Application

IMPLEMENTING INSTRUCTIONS FOR GOAL 4
Reduction and Webification of Applications

1. **Purpose.** To provide implementing guidance for Goal 4 of the Secretary of the Army, Chief of Staff, Army memorandum, Subject: Army Knowledge Management (AKM) Guidance Memorandum Number 2, 3 June 2002 which directs:

   a. "Our goal is to reduce the number of Army Applications by 50 percent by FY2004. AKM Guidance Memorandum Number 1 stated the goal is to link these applications to AKO by July 2002, or obtain a waiver from the Army CIO - this policy is still in effect."

   b. "...HQDA functional proponents and MACOMs will establish a baseline assessment of their applications, streamline the processes associated with these applications, eliminate unnecessary processes/applications and webify appropriate applications."

   c. "By 1 August 2002, all HQDA functional proponents and MACOMs will submit a report to the Army CIO stating their baseline assessments and plans for...reduction and webification of applications. Thereafter, HQDA functional proponents and MACOMs will provide progress reports at Army CIO Executive Board Meetings. "

2. **Guidance Proponent.** The Office of Strategic Partnering, Army Chief Information Officer (CIO) is the proponent for implementation of this guidance. The points of contact for this guidance are LTC Curtis Nutbrown (curtis.nutbrown@us.army.mil, 703-602-7755, DSN 332-7755) and MAJ John Kilgallon (john.kilgallon@us.army.mil, 703-602-3101, DSN 332-3101). The points of contact for Army Knowledge Online are Mr. Charles Cather, Secretary of the AKO CCB, (703-602-2042, DSN: 332-2042, charles.cather@us.army.mil), Colonel Robert Coxe, Chief Technology Officer, (703-704-3623, DSN 654-3623, robert.coxe@us.army.mil), Mr. Robert Schwenk (703-704-3642, DSN 654-3642, robert.schwenk@us.army.mil), and LTC Rod Wade (703-704-3625, DSN 654-3625, roderick.wade@us.army.mil.)

3. **References.**

   a. AKM Guidance Memorandum #1, 8 August 2001.

   b. AKM Guidance Memorandum #2, 19 June 2002.

   c. Joint Technical Architecture-Army (JTA-Army) V6.5, 10 May 2002.

   d. DoDI 5000.2, Change 1, 4 January 2001 - Definitions of mission critical (MC) and mission essential (ME) systems.

   e. AR 25-1, Army Information Management, 31 May 2002 - Incorporates AKM/AKO into Army policy.

4. Definitions.

a. AKO. Army Knowledge Online.

b. AKO-S. Army Knowledge Online-SIPRNet.

c. Application. For the purposes of this document, the terms "application" and "system" are used synonymously - a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. In other words, the application of IT to solve a business problem. System/Application owners will have to use judgment in how to report "systems of systems;" either as a single or separate entries. Standard COTS desktop office automation (i.e. word processors, spreadsheets, etc.) is exempt from the reporting requirements of this document.

d. Army IT Registry Database (AITR). The AITR is an online system, available through the AKO portal to track all Army Systems. Initially, it will focus on tracking webification status for Mission Critical and Mission Essential systems. Eventually, it will be expanded to track all Army systems, and become the single tool for all data calls related to these systems. AITR is available through the AKO portal within the CIO/G-6 Community on the "AKM" page.

e. HQDA Functional Proponent. The functional proponent is typically the HQDA staff element or office, or assistant secretariat responsible for working with the MACOM staffs to develop and validate requirements, determine functional policies and procedures, and fund the development, fielding and operational support of mission systems.

f. Mission Critical (MC) Information System. A system that meets the definitions of "information system" and "national security system" in the Clinger-Cohen Act, the loss of which would cause the stoppage of war fighter operations or direct mission support of war fighter operations. (Note: The designation of mission critical should be made by a Component Head, a CINC or their designee.)

g. Mission Essential (ME) Information System. A system that meets the definition of "information system" in the Clinger-Cohen Act, that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: The designation of mission essential should be made by a Component Head, a CINC or their designee.)

h. System Owner. For the purposes of Goal 4, the owner of a system or application is the MACOM or HQDA functional proponent responsible for the funding, fielding and maintenance of the systems. In the case of these responsibilities being spread across several organizations, the funding organization is the owner unless all the organizations agree on a different owner. If a system is funded by multiple organizations, they will need to pick a single System Owner.

i. Webify. This term encompasses both Web-enabling and Web-basing applications/systems. A Web-enabled system is a system where the user can access information via a thin client browser. A Web-based system has been designed from the ground up so that all functions are performed from any Web browser, including program setup, diagnosis, data entry, report generation, and all other management activities. The following levels of webification, in ascending order, are established for reporting purposes:

1) Web Enabled. System runs on a JTA-Army -approved browser without the need to preload any other software onto the client prior to first web access (software may be downloaded as part of the login).

2) AKO-Linked. System is web enabled and linked through a page on AKO so that users can get to the system via the portal. This is the initial minimum standard that must be met NLT 31 July 2002.

3) AKO Single Sign On. System is AKO-linked and utilizes the AKO Directory Services for access authorization. A user who is logged on to the AKO portal will have access to the system without having to go through a separate system login. The interim goal will be to provide a separate system login prompt that uses the same AKO UserID/password, but this does not count as "AKO Single Sign On" status for reporting purposes.

5. Policy.

a. Webification Waivers. Waivers are needed for any system that will not be webified or will not be linked to AKO by 31 July 2002. Initial waiver authority is delegated to the MACOM and HQDA proponent level. Starting on 1 October 2002, waivers or changes to existing waivers must be approved at the CIO/G-6 level. Waivers cannot be for "indefinite" periods – either a system receives a permanent waiver because webification is not viable, or the waiver must specify the date when the system will be webified. MACOM CIOs and HQDA proponents will enter all waivers and waiver requests into the AITR.

b. Reporting Webification, Waivers and System Reduction: All MACOMs and HQDA proponents will submit written reports to current and future webification and reduction plans on all systems. This report will include the systems of all subordinate activities. MACOMs and HQDA proponents will use AITR to report the webification status and future webification plans of all their IT systems. Initial reports will require status of Mission Critical and Mission Essential systems only. Eventually, all MACOMs/HQDA proponents will report all IT systems status and plans through AITR.

6. Roles and Responsibilities.

a. The Chief Technology Office (CTO), Office of the CIO/G-6 (effective 1 October 2002, moves to U.S. Army Network Enterprise and Technology Command/9th Army Signal Command), as the AKO technical proponent, will:

1) Develop and implement technical architecture for Army-wide AKO account activations and long term AKO services.

2) Provide a means for MACOMs/HQDA proponents to monitor AKO user registration and use sign-in.

3) Provide Help Desk services to facilitate new users.

4) Conduct usage factor analysis with monthly reports to the CIO and HQDA functional proponents and MACOMs.

5) Ensure the capabilities of AKO services are continually refreshed with new technology as the program evolves and technology matures.

6) Provide the AKO Interface Control Document (ICD) outlining the technical procedures to link systems to the AKO directory services for authentication.

7) Develop technical requirements and specifications.

8) Enable Single Sign-On services for webified systems to use for authentication reducing the need for multiple user IDs and passwords.

9) Build the AITR to meet the requirements specified in this document. Share technical documentation with CECOM Software Engineering Center - Ft. Belvoir (SEC-B) within contractual limits.

10) Provide technical data in support of the CIO/G-6 balanced scorecard.

b. The CIO Strategic Partnering Office within the Army CIO/G-6 will:

1) Maintain oversight of waiver policies/criteria for webifying of functional systems.

2) Consolidate, process, and track MACOM/HQDA functional proponent plans and status towards webification of systems

3) Manage the approval process for waiver and proposed changes to MACOM and HQDA functional proponent webification plans.

4) Gather requirements from Army Functional Proponents for incorporation into AKO and AKO-S.

5) Manage the online Army IT Registry database.

c. AKM Directorate within the Army CIO/G-6 as the functional proponent for AKO will:

1) Conduct a Functional Requirements Baseline Analysis and develop and implement a requirements management capability.

2) Determine and integrate enterprise requirements for AKO taking into account HQDA and MACOM requirements.

3) Develop the plans and policies for the development, use, and management of AKO.

4) Develop the taxonomy and information architecture, policy, and procedures for AKO.

5) Develop content life cycle management policies and guidelines for community managers on AKO

6) Develop AKO integrated planning documents and briefings.

7) Assure that all aspects of AKO are adequately addressed in the Army PPBES.

8) Develop and maintain the AKO Management Guide.

d. CECOM Software Engineering Center - Ft. Belvoir (SEC-B) will:

1) Administer the online AITR database to track webification status of Mission Critical and Mission Essential Systems. Act as the AITR Help Desk.

2) Work with MACOMs and HQDA functional proponents to ensure data within the AITR is complete and up to date.

3) Provide input to CIO/G-6 to determine and prioritize improvements to AITR.

4) Provide reports to Army CIO/G-6 and the Army CIO Executive Board on MACOM/HQDA proponent system webification status.

5) Create and maintain an online user's manual for the AITR.

6) Work with CTO to prepare AITR to track all systems (MC, ME and other) NLT 30 September 2002, as well as system elimination/reduction efforts NLT 31 December 2002.

e. HQDA functional proponents and MACOM managers will:

1) Promulgate SEC/CSA Memo to all command levels.

2) Appoint a single POC for all system issues within each MACOM or HQDA proponent. Provide contact information on this individual to Army CIO/G-6 Strategic Partnering NLT 31 July 2002.

3) Webify existing applications/systems and link them to AKO or AKO-S by 31July 2002.

4) Approve MACOM/HQDA system waivers through 30 September 2002. Waivers must be approved at the MACOM CIO or HQDA proponent level.

5) NLT 1 August 2002, submit to CIO/G-6 Strategic Partnering the plan for the reduction and webification of systems. This report should the following information for each system in spreadsheet form: name, description, mission criticality, date system will be webified (see definitions above), reason for waiver (if applicable), and the date any system will be eliminated as part of a reduction effort (if applicable). The report should also project the total number of systems and webified systems by 30 September 04. (Note: this is a paper/e-mail submission, as AITR will not be able to handle non-MC/ME systems by the deadline. MACOMs will be able to download MC/ME system data from AITR in spreadsheet format to be included in this report.)

6) Update the AITR with webification status and future plans of all MC and ME systems NLT 31 August 2002. This includes noting which systems cannot be webified, and the reasons why.

7) Enter all non-MC/ME systems into AITR with webification status, waivers and future plans NLT 31 December 2002.

8) Update your plan for reduction in number of systems to include non-MC/ME systems in AITR NLT 31 March 2003, and keep data current thereafter.

9) Continue procedures for tracking number of AKO users internal to their organizations. Ensure that new members of the organization register for AKO accounts or update their AKO profile as necessary, and that personnel leaving the organization update their AKO profile.

10) Comply with all information assurance and information assurance vulnerability alert requirements.

11) Comply with guidelines contained in the AKO Management Guide (TBP).

12) Where the local implementation of this guidance impacts on bargaining unit employees' conditions of employment, activities are reminded to comply with their statutory and contractual labor relations' obligations.

13) Provide updates at each Army CIO Executive Board on webification status and reduction in total number of systems (systems where the MACOM/functional proponent is the System Owner"). This update should take the form of a single PowerPoint slide. Consolidate systems as Mission Critical, Mission Essential, or "Other", and for each category, report:

a) Total number of systems owned.

b) Number of systems waived from webification.

c) Number of systems webified.

d) Number of systems still to be webified.

e) Number of systems to be eliminated/retired in each of the next three FYs.

f) Number of new systems to be fielded in each of the next three FYs.

7. **Processes.** CONOPS to be published in the AKO Management Guide.

8. **Metrics.**

a. Track MACOM AKO account progress, by numbers and percentages, on a weekly basis (CTO).

b. Track functional webification of MACOM or HQDA proponent systems by mission criticality, number and percentage of systems, on a monthly basis (SEC-B).

c. Track reduction of MACOM or HQDA proponent systems by mission criticality and number (SEC-B).

d. Track MACOM/HQDA proponent utilization of the AITR (SEC-B).

e. Track number of systems using AKO directory services for authentication (eliminating separate userid/passwords) on a quarterly basis (CTO/SEC-B).

f. Track AKO requirements and implementation schedule. Track AKO requirements and implementation schedule (AKM Office).

IMPLEMENTING INSTRUCTIONS FOR AKM MEMORANDUM #2
INFORMATION ASSURANCE

1. Purpose. To provide implementing guidance and instructions for Information Assurance initiatives and status checks as directed by Army Knowledge Management Guidance Memorandum #2, signed by the Secretary of the Amy and the Chief of Staff, Army on 19 June 2002. AKM Guidance Memorandum #2 directs:

> "Each Director of Information Management is responsible for information security at the installation level, but greater connectivity and centralization demands an enterprise approach to security issues, including the Department of Defense's Defense-in-Depth strategy. By August 1, 2002, all HQDA functional proponents and MACOMs will submit a report to the Army CIO on information assurance status and initiatives. The Army CIO, in conjunction with the G-3 and G-2, will provide additional instructions for this report within 30 days as part of the implementing instructions for this memorandum."

2. Guidance Proponent. The Army Chief Information Officer (CIO) in conjunction with the G-2 and G-3 is the HQDA proponent for implementation of this guidance. The points of contact (POC) with the Information Assurance (IA) Division in the Information Operations, Networks and Space Directorate of the Army CIO/G-6 are Chief Sustaining Base Office, LTC John H. Quigg, 703-604-8377, DSN 664-8377, John.Quigg@us.army.mil and IA technical POC, Ralph A. Lowenthal (support contractor), 703-607-5886, DSN 327-5886, Ralph.Lowenthal@us.army.mil.

3. References.

a. AR 380-19, Information Systems Security, 27 February 1998.

b. AKM Guidance Memorandum #1, 8 August 2001.

c. CJCSI 6510.01B Defense Information Operations Implementation Instruction, 22 August 1997 and CJCSI 6510.01B Change 1, Defense Information Operations Implementation instruction Change 1.

4. Definitions.

a. Army Reverse Proxy Server Initiative. Allows access to Army web pages via cached information (proxy server) rather than direct web server access.

b. Backdoors. Connectivity into the installation topology that is not connected IAW Army information assurance standards.

c. Computer Network Defense (CND). Actions taken to protect, monitor, analyze, detect and then respond against unauthorized activity within information systems and computer networks.

d. DITSCAP. DOD Information Technology Security Certification and Accreditation Process.

e. Firewalls. A system designed to prevent unauthorized access to or from a private network.

f. Host-based. Software used on a host computer, either workstation or server, for the benefit of that host only.

g. Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

h. Information Assurance Vulnerability Alert (IAVA). A vulnerability notification and centralized reporting capability for tracking system vulnerability compliance.

i. Intrusion Detection Systems (IDS). A system for detecting attempts to break into or misuse your system.

j. RADIUS. Remote Authentication Dial-In User Server/Service.

k. System Administrator. The person responsible for configuring, administering, and maintaining computers, networks, and software systems.

l. Top Level Architecture, The Army's network security architecture, supported by the Army Signal Command, and located at the networks NIPRNet point of presence.

5. Roles and Responsibilities.

a. The Army CIO will:

1) Act as the Information Assurance functional proponent for all enterprise infostructure initiatives for example (but not limited to) Windows 2000, Active Directory, server consolidation, network management, Public Key Infrastructure, Biometrics, and Common Access Card.

2) Through the Network Enterprise Technology Command (NETCOM), act in concert with the G-2 and G-3 to coordinate CND and Information Assurance

efforts utilizing the defense-in-depth strategy for the Installation Information Assurance Architecture (I2A2) throughout the Army Enterprise Network(s).

b. The HQDA functional proponents, MACOMs, and Regional Installation Management Directors (stood up by 1 October 2002 under the Assistant Chief of Staff for Installation Management) will:

1) Ensure that all applicable IA regulations and policies are followed to protect the Army segment of the Defense Information Infrastructure (DII).

2) Ensure that where applicable all IA-related government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) hardware, firmware, and software components and IT products used in the Army Information Infrastructure have been evaluated and acquired in accordance with National Security Telecommunications Information System Security Policy (NSTISSP) No. 11, and other applicable national and DoD policy and guidance.

6. Process/IA Status and Initiative Assessment (SIA) Requirements. The IA Division developed an Army Knowledge Management IA SIA based in part on requirements from the Deputy Assistant Secretary of Defense DASD for Security and Information Operations CND Assessment Survey. The IA SIA addresses the adequacy of IA policy and resources and overall operational effectiveness. The IA Division survey has been disseminated to MACOM/PEO/PM IA Program Managers (IAPM) for execution. Instructions for completing the IA SIA were disseminated with the assessment. The IA SIA must be completed in two parts. Part I (questions 1 through 4c, 6, and 7 [if interim training information is available]) addresses policy, resources, and operational effectiveness issues. Part II (questions 4d, 5, and 7 [populating the training database]) addresses follow-on requirements. Returning Parts I and II to the Army IA Division is addressed under separate cover. MACOM/PEO/PM IAPMs will ensure that all of their IA Enterprise Assets (question 5), e.g., firewalls, servers, routers, and Intrusion Detection Systems, and IA training information (question 7) are entered into the Army IAVA Compliance Reporting Database (CRD). The IA Division will then evaluate the responses, conduct an in process review on the implementation of the Army's Defense-in-Depth strategy, and develop follow-on recommendations for defending the Army's segment of the DII. The assessment will provide the CIO/G-6 a comprehensive report on the status of the Army's IA posture to include policy, training, resources, and IA operational effectives Army-wide.

7. Metrics.

a. Track MACOM/PEO/PMs responses to the IA/CND Status and Initiative Assessment.

b. Track MACOM/PEO/PMs compliance in entering IA Enterprise Assets and IA training information.